MARYLAND DEPARTMENT OF JUVENILE SERVICES

POLICY

SUBJECT: **Electronic Mail, Internet and Intranet Use Policy**
NUMBER: **IT-1-05 (Information Technology)**
APPLICABLE TO: **Department of Juvenile Services Employees**
EFFECTIVE DATE: **September 20, 2005**

Approved: "/s/ signature on original copy"
Kenneth C. Montague, Jr., Secretary

1. **POLICY.** Electronic mail, Internet and intranet systems are to be used for the execution of a user's job responsibilities in a manner consistent with State standards of business conduct and the mission of each Department of Juvenile Services (DJS) unit. Users shall abstain from illegal, unethical, or other prohibited use of these systems including fraudulent, harassing, threatening, discriminatory, racist, hate-based, lewd, sexually explicit, religious proselytizing, or otherwise disruptive, inappropriate or unauthorized communications, the playing of electronic computer games, and the request for or sharing of information inappropriate to the workplace.

2. **AUTHORITY.**

a. Article 83C, §§2-102 and 2-104.
b. Governor's Executive Order 01.01.2003.01 - Standards of Conduct for Executive Branch Employees.
c. The Maryland Department of Juvenile Services Standards of Conduct and Disciplinary Process.

3. **DEFINITIONS.**

a. *Electronic Mail (e-mail)* means the electronic transfer of information typically in the form of web pages, file transfers, electronic messages, memoranda, and attached documents from a sending party to 1 or more receiving parties via an intermediate telecommunications system. As used in this policy, e-mail includes both the use of DJS's internal mail, GroupWise, and mail through the Internet.
b. *Internet* means a series of computer networks which provide the combined communication pathways of the telephone, mail, television, and radio.
c. *Intranet* means an internal Departmental Internet reference that can be accessed only by authorized users on the Local Area Network (LAN), or Wide Area Network (WAN).
d. *Prohibited Sites* means sites that may elude filtering by the technology protection measures but are nonetheless prohibited. These sites include, but are not limited to, sites relating to chat rooms, entertainment, firearms, bomb making, hacking, sexually explicit, pornographic or nude images or content in any form, gambling, tobacco, alcohol, drugs and unlawful online activities.
e. *Spam* means the widespread distribution of unsolicited email.
f. *User* means any employee, contractual employee or volunteer, or other paid or

unpaid employee who has been granted access to the Internet through the use of the Department's computer network system.

4. PROCEDURES.

a. General Guidelines.

(1) Users shall sign an ***Electronic Mail, Internet, and Intranet Use Agreement*** **(Appendix 1)** acknowledging their understanding of the Department's Policy and Procedure and obligations as a condition of gaining access to a DJS computer network.

(2) Users shall login through the Novell Login screen with their USERID and password every time they start their computer.

(3) Information communicated electronically is subject to State laws, regulations, policies and procedures.

(4) Use of e-mail shall not compromise the integrity of the security of the department's information system.

(5) Use of e-mail for personal gain, to make contacts for private personal gains, or for any illegal or unethical purposes is prohibited.

(6) E-mail addresses, e-mail passwords, equipment and all messages that are created, sent or received using DJS's e-mail systems are the property of the State and may therefore be subject to audit and may be used in legal or disciplinary actions.

(7) Any material which would be inappropriate to be sent on Departmental letterhead is inappropriate for transmission as e-mail and inappropriate for viewing.

(8) All information stored, accessed, or transmitted via DJS electronic systems is subject to monitoring.

(9) The use of the E-mail, Internet, intranet and other State computing equipment, networks, and communication facilities is provided to State employees and contract employees as electronic tools to perform their job functions. Any non work-related access shall be limited to a maximum of 30 minutes per day and may be further limited, prohibited entirely, or restricted to certain times of day by a user's supervisor.

(10) Users shall communicate as they would in a public meeting, and in a professional manner that reflects positively on themselves, the Department, and the State of Maryland.

(11) Users will not (except for authorized Information Technology [IT]

employees):

(i) Grant any unauthorized person access to the e-mail systems without the approval of the Chief Information Officer;
(ii) Access another user's electronic mailbox or read, copy, or alter the contents of another person's mailbox without first obtaining the user's permission;
(iii) Forge or knowingly send forged e-mail messages or attachments to any e-mail message;
(iv) Use profane, obscene, offensive or inflammatory speech in any e-mail message; or
(v) Use the e-mail system to personally attack any individual or entity, share data that is not authorized for distribution or misrepresent oneself, the Department or the State.

(12) Each user with management or supervisory responsibilities shall ensure that users under their supervision are aware of and abide by the obligations under this Policy and Procedure.

(13) All users shall use e-mail, the intranet and the Internet in a professional and productive manner.

(14) Any viewing or attempt to access prohibited sites shall be grounds for disciplinary action.

(15) Any viewing or attempt to access prohibited sites where youth (as defined in the Standards of Conduct and Disciplinary Process and state or federal laws) are inappropriately depicted shall be grounds for immediate termination from the Department and the user may be subject to criminal proceedings.

(16) Access to DJS Internet Services may be revoked, with or without notice if a user violates this Policy and Procedure. In addition, a user may be subject to disciplinary and/or criminal proceedings.

b. Appropriate Usage.

(1) Email and the Internet shall be used for communications that serve legitimate business functions and purposes of the Department and the State of Maryland.

(2) Examples of appropriate use include, but are not limited to:

(i) Communication with federal, state, or local government personnel, vendors, and other private businesses;
(ii) Communication and information exchange for professional development or to maintain knowledge or skills;
(iii) Activities involving public policy associations, government

advisory agencies, or standards activities; and

(iv) Communications for administrative purposes.

c. Prohibited Usage.

(1) Users shall not engage in "chat room" conversations.

(2) Users shall not agree to a license or download any programs without first obtaining the written permission of the Chief Information Officer.

(3) **Internal and External** e-mail may **not** be used for:

(i) Any actions that invade the privacy of individuals or entities that are the creators, authors, users, or subjects of information resources;

(ii) Any communication that does not accurately indicate the true authorized originator and recipient of DJS email communications;

(iii) Attempting to gain access to secure web sites by bypassing the site's security measures (commonly known as "hacking");

(iv) Attempting to gain unauthorized access to any information facility, whether successful or not;

(v) Creating or transmitting threatening, defamatory, fraudulent, annoying, or harassing or otherwise inappropriate messages, even as a prank;

(vi) Disclosing confidential or proprietary information to unauthorized individuals or sending any unauthorized material of a sensitive or confidential nature (i.e. information containing the name, address or Social Security Number of any recipient of DJS services);

(vii) Downloading radio broadcast or music, videos, voice, large graphic files, and lengthy e-mail messages;

(viii) Engaging in any illegal or wrongful conduct, including communications violating any laws or regulations, copyrights, patent protections, license agreements, or other intellectual property rights of third parties;

(ix) Interfering with or disrupting network users, services, or equipment;

(x) Intentionally seeking information about, obtaining copies of, or modifying files, other data, or passwords belonging to other users, unless explicitly authorized to do so by those users;

(xi) Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place excessive load on a computer system or network (such programs are otherwise referred in a variety of ways, including computer viruses, Trojan horses, and worms);

(xii) Knowingly sharing personal information without authorization except as the sharing of personal information is authorized for the care, custody or treatment of youth under DJS supervision;

(xiii) Misrepresenting or concealing in any manner the user's identity, or

other source of transmission of an e-mail or other electronic communication;

(xiv) Private or personal for-profit activities such as consulting for pay, sale of goods, charity fundraising or solicitation of non-State business;

(xv) Running streaming media such as Internet radio and movies;

(xvi) Sending chain letters, spam, letter bombs, advertisements, or commercial solicitations;

(xvii) Viewing or emailing pornographic or sexually explicit materials; or

(xviii) Viewing, playing, or watching other workers play or view any type of computer games or conducting gambling or

(xix) Transmitting e-mail that may reasonably be expected to strain any computing facilities unnecessarily or cause unwarranted or unsolicited interference with others' use of e-mail or e-mail systems.

(xx) Personal or non business related announcements, even when related to DJS employees, unless specifically approved by the Secretary, the Secretary's designee, or the Chief Information Officer.

d. Right to Monitor.

(1) DJS reserves and will exercise the right to review, audit, intercept access and disclose messages or material, including attachments created, received, or sent, Web sites visited and files viewed or downloaded over the Department's electronic mail or Internet systems.

(2) Authorized representatives of DJS may monitor the use of its systems at their sole discretion at any time with or without notice to any user, and may by-pass any password.

(3) A user's work station may be seized and evaluated for inappropriate activity by OPRA or the IT Unit at any given time.

e. Privacy and Confidentiality.

(1) The use of passwords for security does not guarantee confidentiality. Messages and material transmitted and stored on DJS systems are not necessarily confidential. Even when a message or material is erased, it may still be possible to retrieve.

(2) Users are not permitted to retrieve or read e-mail messages that are not sent to them unless their review is authorized by the intended recipient.

(3) Users shall respect client confidentiality in all communications transmitted via e-mail and the Internet and should take all necessary safeguards to protect a youth's right to privacy, including the identification of youth by

first name and last initial followed by a date-of-birth and ISYS or ASSIST identification number.

(4) All Internet messages that contain confidential client information shall be forwarded with the following message attached: "*This electronic transmission may contain confidential or privileged information. If you believe that you have received this message in error, please notify the sender by reply transmission and delete the message without copying or disclosing it. Thank you.*"

f. Representation.

(1) Users may not give the impression that they are representing, giving opinions, or otherwise making statements on behalf of DJS or any unit of the State unless appropriately authorized to do so.

(2) Where appropriate, an explicit disclaimer shall be included unless it is clear from the context of a communication that the author is not representing DJS or the State.

g. Reporting of Inappropriate Usage.

(1) Each user has the responsibility to report any inappropriate usage of e-mail and the Internet.

(2) Users shall report alleged inappropriate usage to their immediate supervisor and the Chief Information Officer.

(3) The Chief Information Officer shall provide to the Director of OPRA a summary of the allegation.

(4) The Director of OPRA shall assign an investigator to investigate any allegation of inappropriate usage.

5. DIRECTIVES/POLICIES AFFECTED.

a. Directives/Policies Rescinded - **None.**

b. Directives Referenced - **None.**

6. FAILURE TO COMPLY.

Failure to obey a Secretary's Policy and Procedure shall be grounds for disciplinary action up to and including termination of employment and the user may be subject to criminal proceedings.

Appendices – 1

1. E-mail Internet, and Intranet Use Agreement

E-MAIL, INTERNET AND INTRANET USE AGREEMENT

I have read the Electronic Mail, Internet and Intranet Use Policy of the Maryland Department of Juvenile Services. I fully understand the terms of this policy and agree to abide by them.

I understand that access to use e-mail, the Internet and the intranet is granted to me by the Department for me to perform authorized duties and responsibilities for the Department. I have no expectations of privacy in connection with my use of the Internet or e-mail system, including sending, receiving or storing information. I understand that all information stored, accessed or transmitted is subject to monitoring and that management reserves the right to examine, copy or archive files, transmission, or e-mails.

By signing this agreement, I certify that I understand the terms and conditions of this agreement and that I accept responsibility for adhering to the agreement. I also acknowledge my understanding that any infractions on my part may result in disciplinary action.

Printed Name of Employee _____

Signature of Employee _____

Date: _____

MARYLAND DEPARTMENT OF JUVENILE SERVICES
EMPLOYEE STATEMENT OF RECEIPT
POLICY AND PROCEDURE

SUBJECT: Electronic Mail, Internet and Intranet Use Policy
POLICY NUMBER: IT-1-05 (Information Technology)
EFFECTIVE DATE: September 20, 2005

I have received one copy (electronic or paper) of the Policy and/or Procedure as titled above. I acknowledge that I have read and understand the document, and agree to comply with it.

_____ _____
SIGNATURE PRINTED NAME

_____
DATE

(THE ORIGINAL COPY MUST BE RETURNED TO YOUR IMMEDIATE SUPERVISOR FOR FILING WITH PERSONNEL, AS APPROPRIATE.)